Matrix Power S-Box Construction*

Eligijus Sakalauskas[a] and Kestutis Luksys[b]
Department of Applied Mathematics,
Kaunas University of Technology, Studentu g. 50, 52368 Kaunas, Lithuania
[a]Eligijus.Sakalauskas@ktu.lt [b]Kestutis.Luksys@ktu.lt

Abstract

The new symmetric cipher S-box construction based on matrix power function is presented. The matrix consisting of plain data bit strings is combined with three round key matrices using arithmetical addition and exponent operations. The matrix power means the matrix powered by other matrix. The left and right side matrix powers are introduced. This operation is linked with two sound one-way functions: the discrete logarithm problem and decomposition problem. The latter is used in the infinite non-commutative group based public key cryptosystems. It is shown that generic S-box equations are not transferable to the multivariate polynomial equations in respect of input and key variables and hence the algebraic attack to determine the key variables cannot be applied in this case. The mathematical description of proposed S-box in its nature possesses a good "confusion and diffusion" properties and contains variables "of a complex type" as was formulated by Shannon.

Some comparative simulation results are presented.

Keywords: symmetric cipher, S-box, matrix power, one-way function (OWF), resistance to algebraic attack

1 Introduction

As it is known, the design criteria for the block ciphers as for other cryptographic systems are related with the known cryptanalytic attacks. It is essential that after the new attack invention the old design criteria must be changed. The new attack is the algebraic attack declared in (Schaumuller – Bihl, 1983) and developed in (Courtois and Pieprzyk, 2002).

The old design criteria were oriented to the most powerful attacks such as linear and differential and were successfully satisfied for the several known ciphers, for example AES, Serpent, Camellia Misty/Kasumi etc. It was shown that the non-linearity properties of the inverse function in $GF(2^n)$ used as a single non-linear component in AES are close to optimality with respect to linear, differential and higher-order differential attacks (Canteaut and Videau, 2002).

But nevertheless it is shown that many known "optimal" ciphers have a very simple algebraic structure and are potentially vulnerable to the algebraic attack (Courtois and Pieprzyk, 2002). The vulnerability is related to S-box description by implicit input/output and key variables algebraic equations of polynomial type. For example the AES can be described by the system of multivariate

*Work supported by the Lithuanian State Science and Studies Foundation

quadratic equations in $GF(2^8)$ for which the XL or XSL attack can be applied in principle. The algebraic cryptanalysis methods are based on the creation of overdefined system of algebraic equations describing the cipher's input/output variables and the round key. It is required the equations to be of polynomial type. Then there is a principal opportunity to find the solution of these equations by some feasible algorithm that might be of sub-exponential time and recover the key from a few plaintext/ciphertext pairs.

The algebraic attack changes some old security postulates (Courtois, 2005):

1. The complexity is no longer condemned to grow exponentially with the number of rounds.
2. The number of required plaintexts may be quite small (e.g. 1).
3. The wide trail strategy should have no impact whatsoever for the complexity of the attack.

Despite the fact that there are no practical results of breaking the entire AES by algebraic attack yet, it is sensible to build the new design methods possessing a higher resistance to algebraic attack. According to Courtois the design of ciphers will never be the same again and this is supported by the declared new ideas for the S-box construction laying on the sufficiently large random S-boxes to prevent all algebraic attacks one can think (Courtois et al., 2005).

The other helpful ideas could be found by looking back to the origin (Shannon, 1949). According to Shannon, the complexity of breaking a secure cipher should require "*... as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type*".

We would like to present here a certain interpretation and realization of Shannon, Courtois and Pieprzyk complexity vision. In general, it is desirable the complexity of solving a system of equations to be at least NP-hard. We propose here a certain S-box construction where input and key variables seems to be "*of a complex type*" since the equations containing these variables are not an algebraic ones. We think that Shannon's principle of confusion and diffusion is also realized in our S-box construction. It is related with the mixing principle of ergodic theory and can be realized by two non-commutative operations. Actually the same is done in our S-box construction.

According to (Impagliazzo and Luby, 1989) with given any secure private key encryption scheme one can construct a one-way function (OWF). The following theorem was proved (Goldwasser and Bellare, 2001): there exists a secure private key encryption scheme if and only if there exists a one-way function.

With reference to this theorem we would like to present S-box construction for the symmetric key cipher. The starting point is a particular OWF postulation. Further this OWF is used for the S-box construction.

One of postulated and traditional OWF is the modular exponent which inversion corresponds to the discrete logarithm problem (DLP) (Menezes et al., 1997). We present here some generalization of this OWF using a matrix group action problem in vectorial Galois field $GF^m(2^n)$. The idea to use the group or semigroup action problem in vectorial spaces for the asymmetric cryptographic primitives' construction can be found in (Monico, 2002). We have generalized this approach and applied it to our S-box construction. As a result we have obtained some OWF which is linked not only with a classical DLP but also with so called decomposition problem (DP), used in the asymmetric cryptosystems based on the hard problems in infinite non-commutative groups (Shpilrain and Ushakov, 2005). The same kind of DP is used also in two digital signature schemes construction (Sakalauskas, 2004) and (Sakalauskas, 2005).

We use the procedure of cipher key expansion to the round key and the latter is a little more than three times longer than the plain data block. Key schedule can be realized by the pseudo random number generator. The round key consists of three matrices. One of them is over $GF(2^{n-1})$ and two of them are over $GF(2^n)$. The latter matrices must be invertible. Some remarks on this issue are presented in section 5.

The presented S-box is investigated with respect to the algebraic cryptanalysis (Courtois and Pieprzyk, 2002). It is shown that the equations describing the S-box input/output and round key variables are not polynomial and hence the XL or XSL methods do not suit in this case.

Some simulation results are presented for low dimensional example which is compared with known APN power functions of Gold, Kasami and inverse type.

2 Preliminaries

Let us consider a set of binary strings of length $(n-1)$ denoted by $F_2^{n-1} = \{0,1\}^{n-1}$. The arithmetic addition operation between two strings can yield the string of the same length or of the length n. For example when $n = 3$, $a = 01$ and $b = 10$ the arithmetic addition of a and b gives 11, i.e. $01 + 10 = 11$. If $a = 11$, then $a + b = 11 + 10 = 101$.

The set $F_2^n = \{0,1\}^n$ we can interpret as n-dimensional vector space over $F_2 = \{0,1\}$. According to (Logachev et al., 2004) there is a natural isomorphism between the F_2^n and Galois field $GF(2^n)$. Hence any element $a \in F_2^n$ we interpret in the following ways: as an integer number represented by the binary string; as an element of a vector space F_2^n; and as an element of $GF(2^n)$. The chosen interpretation will be clear from the context.

Let us define a $m \times m$ matrices over $GF(2^n)$. The set of all matrices over $GF(2^n)$ we denote as M. We do not introduce any internal operations in the set M. For further considerations we are interested only in external operations performed in this set.

Let $M_G \subset M$ be a group of matrices over $GF(2^n)$ with the commonly defined matrix multiplication operation and matrix inverse.

We now introduce a matrix group M_G left and right action operations in the set M, denoted by $\circ_L$ and $\circ_R$ respectively. In a formal way $\circ_L$ is a mapping $\circ_L : M_G \times M \to M$ and $\circ_R : M \times M_G \to M$. Then $\forall L, R \in M_G$ and $\forall X \in M$ there exist some $Y, Z \in M$ such that $L \circ X = Y$ and $X \circ R = Z$. Further for the simplicity the symbols $\circ_L$ and $\circ_R$ are omitted and replaced by the common action operation $\circ$ which assignment to $\circ_L$ and $\circ_R$ is clear from the context.

The elements of matrices L, X, R, Y, Z we denote by the indexed set of its elements respectively, e.g. by $\{x_{ij}\}$ we denote matrix X.

We have chosen the following action operations which can be written for the matrix equation $L \circ X = Y$ elements

$$y_{ij} = \prod_{s=1}^{m} x_{sj}^{l_{is}}, \tag{1}$$

and for the matrix equation $X \circ R = Z$ elements

$$z_{ij} = \prod_{t=1}^{m} x_{it}^{r_{tj}}. \tag{2}$$

The multiplication and power operations are performed using $GF(2^n)$ arithmetics.

Example 1. To give a simple example, let us assume that matrices have two rows and two columns, i.e. $m = 2$.

In this case, matrix Y can be expressed in the following way

$$Y = L \circ X = \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \circ \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} x_{11}^{l_{11}} x_{21}^{l_{12}} & x_{12}^{l_{11}} x_{22}^{l_{12}} \\ x_{11}^{l_{21}} x_{21}^{l_{22}} & x_{12}^{l_{21}} x_{22}^{l_{22}} \end{pmatrix}.$$

Matrix Z can be expressed in the following way

$$Z = X \circ R = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \circ \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} = \begin{pmatrix} x_{11}^{r_{11}} x_{12}^{r_{21}} & x_{11}^{r_{12}} x_{12}^{r_{22}} \\ x_{21}^{r_{11}} x_{22}^{r_{21}} & x_{21}^{r_{12}} x_{22}^{r_{22}} \end{pmatrix}.$$

3 S-box construction

The S-box input data we denote by matrix D with elements being binary strings in vector space F_2^{n-1}. Using the certain key expansion procedure we can generate the round keys: matrix K over F_2^{n-1} and matrices $L, R \in M_G$. Input/output and key matrices are all of the same $m \times m$ size.

S-box transformations of input data D to ciphered output data C are performed as following

$$D + K + \mathbf{1} = X, \tag{3}$$

$$L \circ X \circ R = C, \tag{4}$$

where $D + K + \mathbf{1}$ denotes the arithmetical addition of matrices with elements of binary strings in F_2^n; $\mathbf{1}$ is the matrix consisting of arithmetical unity elements in F_2^n. Combining (3) and (4) we obtain

$$L \circ (D + K + \mathbf{1}) \circ R = C, \tag{5}$$

From (3) we obtain a matrix $X \in M_Z$ which does not contain zero elements, i.e. is without zero binary strings. By left-right action of matrix X with matrices $L, R \in M_G$ we obtain a ciphered data C being a matrix in M_Z. We can write now the implicit formula for an element c_{ij}

$$c_{ij} = \prod_{t=1}^{m} \prod_{s=1}^{m} x_{st}^{l_{is} \cdot r_{tj}} = \prod_{t=1}^{m} \prod_{s=1}^{m} (d_{st} + k_{st} + 1)^{l_{is} r_{tj}} \tag{6}$$

where 1 is a bit string corresponding to arithmetical unit in F_2^n.

Since M_G is a group of matrices, then there exists the inverse matrix R^{-1} such that $RR^{-1} = R^{-1}R = I$, where I is the identity matrix. Then instead of using R we will use the R^{-1} for the symmetry in this section.

The encryption operator corresponding to this S-box and depending of the round keys K, L, R^{-1} we denote by $E_{R'LK}$. Symbolically, using (6), the encryption procedure can be written by the relation

$$E_{R'LK}(D) = C. \tag{7}$$

Example 2. Continuing previous example ciphered data matrix can be expressed like this one

$$C = L \circ (D + K + \mathbf{1}) \circ R' =$$

$$= \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \circ \left(\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} + \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right) \circ \begin{pmatrix} r'_{11} & r'_{12} \\ r'_{21} & r'_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \circ \begin{pmatrix} d_{11} + k_{11} + 1 & d_{12} + k_{12} + 1 \\ d_{21} + k_{21} + 1 & d_{22} + k_{22} + 1 \end{pmatrix} \circ \begin{pmatrix} r'_{11} & r'_{12} \\ r'_{21} & r'_{22} \end{pmatrix},$$

here D is a S-box input data (plain data) matrix. From this expression we can express the cipher data matrix elements

$$c_{11} = (d_{11} + k_{11} + 1)^{l_{11}r'_{11}} (d_{12} + k_{12} + 1)^{l_{11}r'_{21}} (d_{21} + k_{21} + 1)^{l_{12}r'_{11}} (d_{22} + k_{22} + 1)^{l_{12}r'_{21}},$$

$$c_{12} = (d_{11} + k_{11} + 1)^{l_{11}r'_{12}} (d_{12} + k_{12} + 1)^{l_{11}r'_{22}} (d_{21} + k_{21} + 1)^{l_{12}r'_{12}} (d_{22} + k_{22} + 1)^{l_{12}r'_{22}},$$

$$c_{21} = (d_{11} + k_{11} + 1)^{l_{21}r'_{11}} (d_{12} + k_{12} + 1)^{l_{21}r'_{21}} (d_{21} + k_{21} + 1)^{l_{22}r'_{11}} (d_{22} + k_{22} + 1)^{l_{22}r'_{21}},$$

$$c_{22} = (d_{11} + k_{11} + 1)^{l_{21}r'_{12}} (d_{12} + k_{12} + 1)^{l_{21}r'_{12}} (d_{21} + k_{21} + 1)^{l_{22}r'_{12}} (d_{22} + k_{22} + 1)^{l_{22}r'_{22}}.$$

Formally the decryption operator is $E^{-1}_{R'LK} = D_{K'L'R}$. We can write the following relations for deciphering

$$\begin{aligned} &D_{K'L'R}(C) = D_{K'L'R}(E_{R'LK}(D)) = \\ &= D_{K'L'R}(L \circ (D + K + \mathbf{1}) \circ R^{-1}) = \\ &= D_{K'L'}(L \circ (D + K + \mathbf{1}) \circ R^{-1} \circ R) = \\ &= D_{K'L'}(L \circ (D + K + \mathbf{1})) = \\ &= D_{K'}(L^{-1} \circ L \circ (D + K + \mathbf{1})) = \\ &= D_{K'}(D + K + \mathbf{1}) = \\ &= D + K + \mathbf{1} - K - \mathbf{1} = D. \end{aligned}$$

We have obtained that

$$D_{K'L'R}(C) = D, \tag{8}$$

when assumed that indexes L' and R' act as matrices L^{-1} and R^{-1} respectively and K' is expressed as additive inverse, i.e. as $(-K - \mathbf{1})$ matrix.

For the validity of last equations the left-right action operations must satisfy the following properties:

1. The action operations must be associative, i.e.

$$L \circ (X \circ R) = (L \circ X) \circ R.$$

2. The action operations are both left and right invertible, i.e.

$$L^{-1} \circ (L \circ X) = (L^{-1}L) \circ X = I \circ X = X,$$

$$(X \circ R^{-1}) \circ R = X \circ (R^{-1}R) = X \circ I = X.$$

Theorem 1. The action operations are associative.

Theorem 2. The action operations are both left and right invertible.

The proof of these theorems follows from the equation (6), matrix multiplication rule and inverse matrix definition.

So we have defined valid encryption-decryption operators.

4 The security considerations

Security was considered from two points of view. The first one is a consideration of generic S-box equations and their natural link with some sound one-way functions used in asymmetric cryptography. The second one is the security analysis against known cryptanalytic attacks to the block ciphers.

The proposed S-box uses the generalization of traditional modular exponent function which is recognized as an OWF.

Some generalization of modular exponent is presented in (Monico, 2002) by introducing a group or semigroup action operation in vector space. According to the author, the inverse action problem is harder than classical DLP. Hence when using this group action problem we can reduce the value of prime p for the Galois field $GF(p)$.

In this paper we generalized the approach presented in (Monico, 2002) by introducing a left-right group M_G actions in the matrices set M, as matrix powers functions on elements of M. In other words the matrix in M is powered by matrix from M_G. The powering can be performed either from the left or from the right side.

This action can be treated as a generalization of both classical DLP and DLP presented in (Monico, 2002). The introduced action operation we name a matrix power and related OWF as matrix power OWF. Then the OWF inversion problem might be called correspondingly as matrix power DLP.

It can be seen that the constructed matrix power OWF is linked with the other kind of hard problem known as decomposition problem (DP) in cryptosystems based on the infinite non-commutative groups (Shpilrain and Ushakov, 2005). The examples of using DP in the digital signature schemes based on infinite non-commutative group representation level can be found in (Sakalauskas, 2004) and (Sakalauskas, 2005). Using our notations, this problem can be stated as follows: by having X and C in M, find L and R in M_G from (4). Hence this DP is not equivalent to the classical matrix DP. The introduced DP we call the matrix power DP. Then the security of constructed S-box relies on the two simultaneous problems: the classical DLP and matrix power DP.

To determine the secret keys an adversary must simultaneously solve the system of (3) and (4) matrices equations. The first equation is a linear, and the second one is a non-linear equation with a simultaneous solution of classical DLP and matrix power DP.

Let us discuss the second approach of security consideration. We do not theoretically consider the linear, differential or higher order differential attacks for the proposed S-box. First of all our aim is to investigate the proposed S-box security against algebraic attack. The idea of algebraic attack was presented in (Shaumuller – Bihl, 1982). The development of algebraic attack for some known block ciphers, i.e. AES, Serpent, Camellia etc., was presented in (Courtois and Pieprzyk, 2002). As it is known the algebraic attack is based on S-box description by algebraic equations relating plain data, cipher data and round keys. In general, the algebraic attack is applied to S-box modeled as discrete input/output system described by the system of algebraic relations. The aim

of algebraic attack is to find a key variables by solving the S-box system of equations having one or more plaintext/ciphertext pairs.

For example the algebraic structure was constructed for AES and other ciphers (Murphy and Robshaw, 2002), (Courtois and Pieprzyk, 2002), (Murphy and Robshaw, 2003), (Biryukov and Canniere, 2003), (Cheon and Lee, 2004), (Courtois, 2004), (Courtois et al., 2005).

The main mathematical tools for the algebraic cryptanalysis are the XL algorithm (Courtois et al., 2000) and its improved version – the XSL algorithm (Courtois and Pieprzyk, 2002) and (Cid and Leurent, 2005). These methods are using the simple generic algebraic structure of ciphers listed above. For example AES applies the inverse exponent function and hence can be described by the overdefined multivariate quadratic polynomial system of equations. The XL (XSL) method allows the construction of overdefined system of equations which can be solved by the linearization method. Despite the conjecture that the solution of obtained system of equations is NP-hard, but nevertheless the algebraic attack has a great potential threat to the ciphers listed above.

Let us turn again to the system (6) of m^2 equations. We can say that to perform the XL (XSL) attack this system must be transformed to certain system of multivariate polynomial equations. Let us consider the problem to obtain a system of multivariate polynomial equations with respect to the key variables. Each equation in (3) provides an injective mapping $F_2^{n-1} \times F_2^{n-1} \to F_2^n \backslash \{0\}$, where $F_2^n \backslash \{0\}$ is the set F_2^n without zero element.

The system of equations defined by matrix equation (5) contains the (6) type of equations. It is evident that those equations are not polynomial with respect to the key variables l_{is}, r_{tj} and k_{st}. there is no transformation to obtain a system of polynomial equations with respect to the key variables from (5). Hence the XL (XSL) methods and as a consequence the conventional algebraic attack cannot be applied when the pair of plain/cipher data $D = \{d_{st}\}$ and $C = \{c_{ij}\}$ is known.

Due to the fact that generic S-box equations are not vulnerable to the recently invented algebraic attack, there is no sense to speak about its algebraic immunity as defined in by Courtois and Pieprzyk. But nevertheless it is interesting to compare the complexity of presented S-box with other ones using several convenient criteria. We perform this comparison by considering our S-box as a vector Boolean function by evaluating its algebraic normal form (ANF), estimating its non-linearity and other cryptographic criteria. This investigation does not provide the exhausting information about the S-box security since these equations do not contain round key variables, but only input/output relations. Moreover, vector Boolean functions could be constructed only for the small dimension example. We considered a Matrix power S-box having 8 inputs and 12 outputs. This corresponds to the values $m = 2$ (number of rows and columns) and $n = 3$. For each our S-box realization we chose the concrete matrices K, L and R of order 2×2 and generated the vector Boolean functions truth table and ANF for all $m^2 n = 12$ outputs. We randomly selected four Matrix power S-boxes denoted by Matrix power 1-4.

First of all the main two criteria characterizing the resistance to the linear and differential cryptanalysis were calculated: differential potential and non-linearity (Pommerening, 2005), (Logachev et al., 2004). These criteria were also calculated for the following known exponential functions: Gold, Kasami and inverse (Courtois et al., 2005). The S-boxes corresponding to these exponents have 8 inputs and 8 outputs. All the computations were done in $GF(2^8)$. The calculation results are presented in Table 1.

As it seems, the two traditional resistance criteria of exponent S-boxes are better than the Matrix power S-boxes. It is no surprise, since Gold, Kasami and inverse exponents are near to optimal with respect to these criteria and are the representatives of almost perfect nonlinear (APN) functions.

S-box	Exponent power	Differential potential	Non-linearity
Gold	17	0.008	112
Kasami	241	0.063	104
Inverse	253	0.016	112
Matrix power 1	-	0.047	92
Matrix power 2	-	0.063	94
Matrix power 3	-	0.078	94
Matrix power 4	-	0.055	94

Table 1: The comparative cryptographic criteria of different S-boxes

S-box	Term degree						
	2	3	4	5	6	7	8
Gold	23%	8%	6%	1%	0%	0%	0%
Kasami	50%	51%	47%	45%	28%	8%	0%
Inverse	55%	47%	48%	48%	46%	47%	0%
Matrix power 1	43%	50%	44%	51%	43%	23%	0%
Matrix power 2	46%	51%	47%	52%	48%	45%	8%
Matrix power 3	51%	50%	43%	51%	46%	52%	0%
Matrix power 4	46%	48%	41%	51%	49%	48%	8%

Table 2: The average non-linear terms percentage in ANFs of 8 bits S-boxes

The other way to estimate the non-linearity of S-box expressed by vector Boolean function is to calculate the average number of non-linear terms presented in each ANF of each degree, beginning from the second. The average is taken for all ANFs corresponding to different outputs. The calculation results are presented in Table 2.

As it seems the average non-linear terms number of high degree is the highest in Matrix power S-boxes. For example, the 8% of terms of the highest degree 8 shows that among 12 outputs of Matrix power S-box this term presents in 1 output.

The number of rows of Matrix power S-box Boolean function truth table is $2^{m^2(n-1)}$ and hence we cannot choose the next toy example for $m = 3$ and $n = 4$. The truth table will have 2^{27} rows and this is more than the computational limit of 2^{25} for the calculation of listed above cryptographic criteria.

5 Implementation

The main problem for the S-box implementation is to generate random round key matrices L and R having their inverses from the cipher key. There are a lot of means to solve this problem with different computation efficiency. One of the method is to use the certain non-commutative group

representation in the set of matrix group $GL(m, GF(2^n))$. The non-commutative group is presented by finite sets of generators and relations. Then it is required to construct representation matrices and their inverses for each initial group generator.

For random round key generation the random group element (word) is generated and is expressed in the terms of group generators. The pseudo random number generator can be applied. If the matrix L is required to be obtained then the group word is transformed to the matrix L by the representation homomorphism. If the inverse matrix R^{-1} is required then the inverse group word is taken and R^{-1} is obtained by applying the representation homomorphism to the inverse word. These operations are computationally effective.

We do not consider this problem in detail and postpone this construction to be described in the next papers.

The security parameters of our S-box are m (size of matrices) and n (length of binary strings). We reckon that the values of parameter m from the set $\{4, 5, 6, 7, 8\}$ and the values of n from the set $\{8, 16, 32\}$ could be computationally effective. The higher the values of m and n, the fewer matrix power S-boxes are required for the cipher. We think that for $m = 8$ and $n = 32$ the application of one round could be enough.

6 Discussion

We think that proposed S-box construction is resistant for the recent algebraic attack due the complex type of its generic equations having relations with known OWFs.

We can also notice that in essence this S-box construction simply must guarantee a good Shannon's confusion and diffusion properties. This is achieved due to the left-right matrix group action introduction in the form of matrix power. As a result a large number of unknowns of a complex type in the generic S-box relations are also presented.

References

[1] A. Biryukov, C. Canniere. Block Cipher and Systems of Quadratic Equations. Proceedings of FSE'2003, LNCS 2887, pp. 274-289, 2003.

[2] A. Canteaut, M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. Advances in Cryptology Eurocrypt'2002, Springer Verlag 2002.

[3] J.H. Cheon, D.H. Lee. Resistance of S-boxes against Algebraic Attacks. Fast Software Encryption, LNCS 3017, pp. 83-94, Springer-Verlag, 2004.

[4] C. Cid, G. Leurent. An Analysis of the XSL Algorithm. ASIACRYPT 2005, LNCS 3788, pp. 333-335, 2005.

[5] N.T. Courtois. General Principles of Algebraic Attacks and New Design Criteria for Cipher Components. Advanced Encryption Standard – AES, LNCS 3373, pp. 67-83, 2005.

[6] N.T. Courtois, B. Debraize, E. Garrido. On exact algebraic [non-]immunity of S-boxes based on power functions. Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/203, 28 June, 2005.

[7] N.T. Courtois, J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Proceedings of Asiacrypt'2002, LNCS 2501, pp. 267-287, Springer-Verlag , 2002.

[8] N.T. Courtois. Feistel Schemes and Bi-Linear Cryptanalysis. Advances in Cryptology – CRYPTO 2004, LNCS 3152, 2004.

[9] N.T. Courtois, A. Klimov, J. Patarin, A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. Eurocrypt'2000, LNCS 1807, pp. 392-407, 2000.

[10] C.W. Curtis. Representation theory of finite groups and associative algebras. John CityWiley State& StateSons, StateNew York, placeCityLondon, 1962.

[11] S. Goldwasser, M. Bellare. Lecture Notes on Cryptography. 2001. *http://theory.lcsmit.edu/shafi*

[12] R. Impagliazzo, M. Luby. One-way functions are essential for complexity based cryptography. In Proc. 30th IEEE Symp. on Foundations of Comp. Science, 1989.

[13] O.A. Logachev, A.A. Salnikov, V.V. Yaschenko. Boolean functions in coding theory and cryptography (in russian). M.: McNNO, 2004.

[14] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[15] C. Monico. Semirings and Semigroup actions in Public–Key Cryptography. PhD. thesis, University of Notre Dame, May 2002.

[16] S. Murphy, M.J.B. Robshaw. Comments on the Security of the AES and XSL Technique. Electronic Letters, Vol. 39, pp. 26-38, 2003.

[17] S. Murphy, M.J.B. Robshaw. Essential Algebraic Structure Within the AES. Proceedings of CRYPTO 2002, LNCS 2442, pp.1-19, Springer-Verlag, 2002.

[18] Pommerening K. *Fourier Analysis of Boolean Maps – A Tutorial.* 2005. Available at: http://www.staff.unimaiz.de/pommeren/kryptologie/bitblock/a-nonlin/fourier.pdf.

[19] E. Sakalauskas. New Digital Signature Scheme in Gaussian Monoid. *Informatica*, ISSN: 0868-4952, 2004, Vol. 15, No. 2, p. 251-270.

[20] E. Sakalauskas. One Digital Signature Scheme in Semimodule over Semiring. *Informatica*, ISSN: 0868-4952, 2005, Vol. 16, No. 3, p. 383-394.

[21] Schaumuller-Bichl. Cryptanalysis of the Data Encryption Standard by the Method of Formal Coding. Advances in Cryptology EUROCRYPT-1982, LNCS 149, pp.235-255, Springer-Verlag, 1983.

[22] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26, 1997, p.1484-1509.

[23] V. Shpilrain and A. Ushakov. A new key exchange protocol based on the decomposition problem. 2005. // Available at: http://eprint.iacr.org/2005/447.